Giornata AA - GARR
Roma, Italy
07 March 2007

<Licia Florio>

<TERENA >

licia@terena.org

www.terena.org

Overview of Middleware Developments in Europe

Outline

- Why Federated Identity Management
- Federation concepts
- European landscape in higher education
- TERENA’s role
- A quick look at the future

Identity Management

- A step back:
  - Identity Management
    - Giving each user an electronic identity
    - Set of technologies and policies to control users access to resources
- Plenty of Identity Management Systems available
  - Open source
  - Proprietary
  - More or less sophisticated, depending on the needs

The Needs For Federated Identity Management

- Increasing dynamics in the education system
  - Students can access courses in other faculties
  - Students take some course units abroad
  - On-line courses are more common
  - Users want to access the same services no matter where they are
  - Grid: example of access to distributed resources

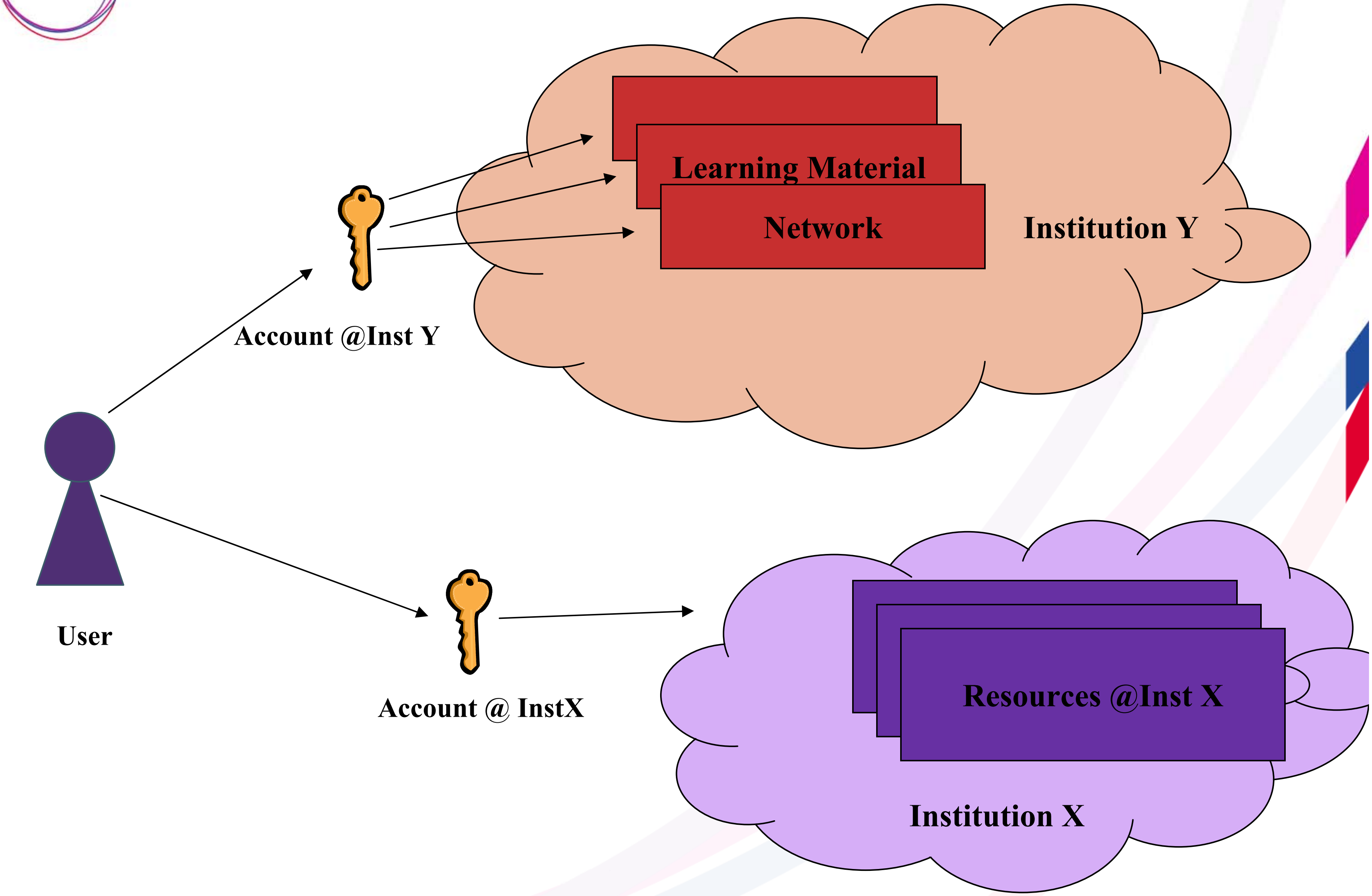
- More institutions dealing with the same users means:
  - Multiple registration of users
  - Overhead to manage guest users
  - Increased possibility of error in managing the users' records

What Federated Identity Management Offers

- Federated Identity Management allows institutions to exchange users' data
  - Beyond the institutional borders
- Federated Identity Management allows cross-institutional service provisioning
  - No redundant data for the institutions: the users' data is provided by user home institution
  - No extra accounts needed: the users can login with the credentials provided by their home institutions

The provision of a service is based on the authentication performed by the home institution (SSO)

Example of Not Federated Access



Learning Material

Network

Institution Y

Account @Inst Y

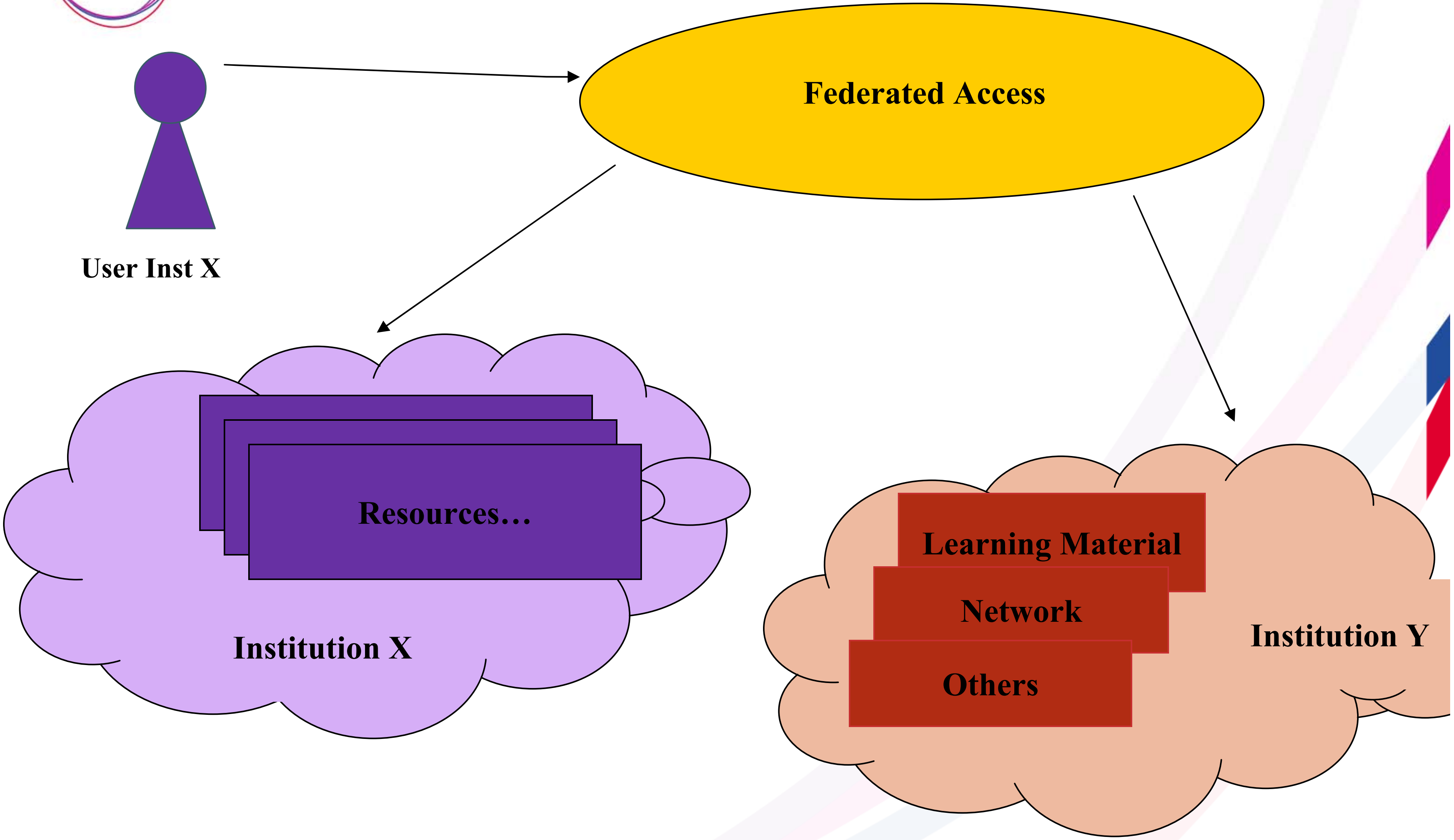
User

Account @ InstX

Resources @Inst X

Institution X

Example of Federated Access



Federated Access

User Inst X

Resources…

Institution X

Learning Material

Network

Others

Institution Y

Terminology

- Identity Provider
  - The organisation that performs the identity verification for the users
  - For resources belonging to the same organisation
  - For resources belonging to other organisations (that part of the federation;

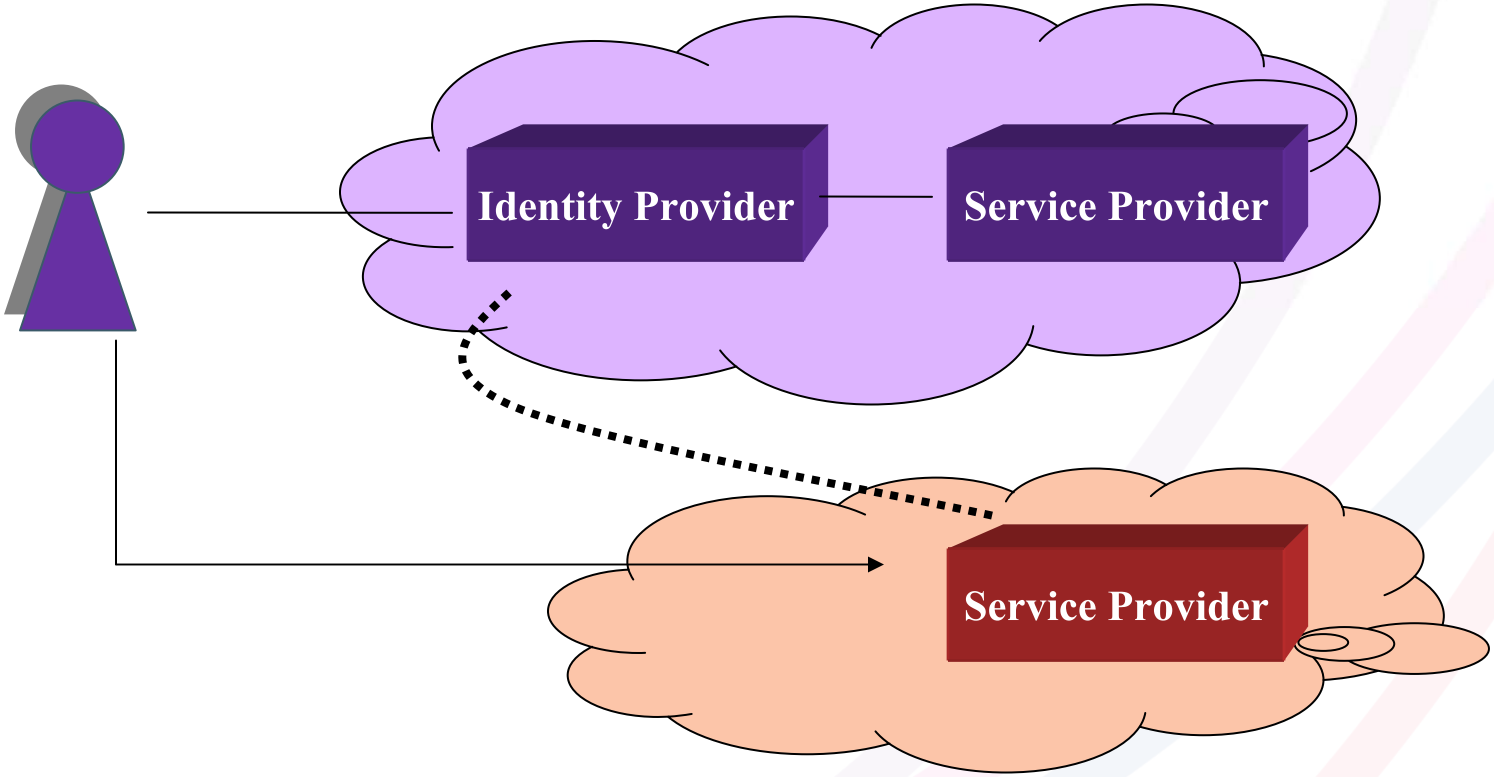
- Service Provider
  - The service offered to the user based on the authentication provided by the Identity Provider

Federations

- Enable the sharing of educational resources
  - Network
    - Wireless and/or not
  - Applications
    - Online learning systems

- Require agreement on:
  - Legal Framework and Policies
    - Trust
  - Technology
    - Security
  - Common Language
    - Interoperability

The Building Blocks of Federations



Higher Education European Landscape

- Federations are being developed at national level by the NRENs
- Different (open source) solutions are used
  - Shibboleth: UK, Finland, Switzerland
  - PAPI: Spain
  - A-Select: the Netherlands
  - Sun Federation Manager based upon Liberty Alliance specification: Norway

- All these solutions are now inter-operable

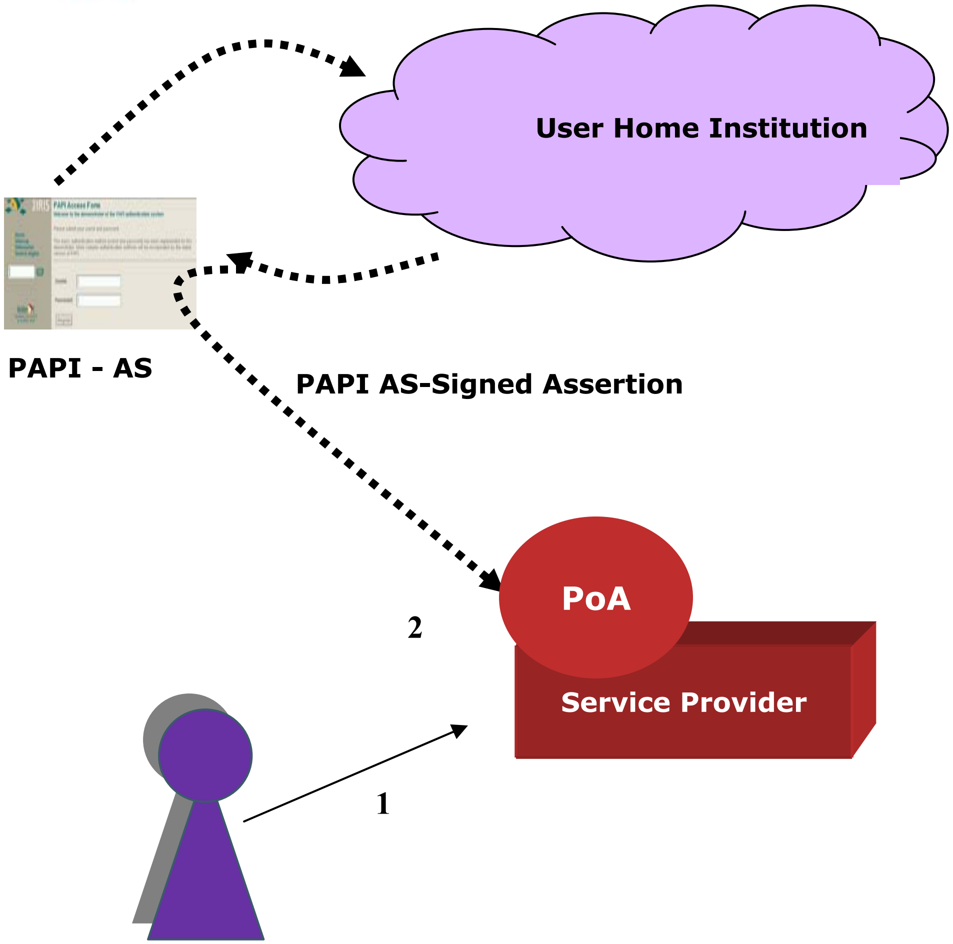
- They all recognize Security Assertion Markup Language (SAML) as “the standard” to transfer information (assertions) among each other

SSO Systems: PAPI

- PAPI Components:
  - The Authentication Server (AS) => IdP
    - Provides users with a (local) single authentication point
    - Source for user attribute data
  - The Point of Access (PoA) => inner SP
    - Performs actual access control for a given organisation
    - Uses temporary cryptographic tokens, encoded as HTTP cookies
  - The Group Point of Access (GPoA) => outer SP
    - Combines a group of PoAs with similar access policies
    - Intended to simplify AS-PoA interactions and PoA operation

Courtesy of Diego Lopez (RedIRIS)

PAPI Scenario



- User logs in via the PAPI-AS
  - Different AuthN mechanism can be used
- Upon login the user gets a list of authorized locations (URLs)
- The browser contacts the sites
- PoA performs the authZ

What PAPI Offers

- Covers both
  - Web SSO (intra-institutional): PAPI protocol
  - Federations (inter-institutional): PAPI protocol plus Shibboleth SAML profiles
- Simpler to deploy once the outer services are in place
- Binding for several application languages
  - Perl
  - Java (JAAS, Servlet filter and JNLP)
  - PHP
- Proxy mode for legacy resources

Courtesy of Diego Lopez (RedIRIS)

Connecting PAPI and Shibboleth

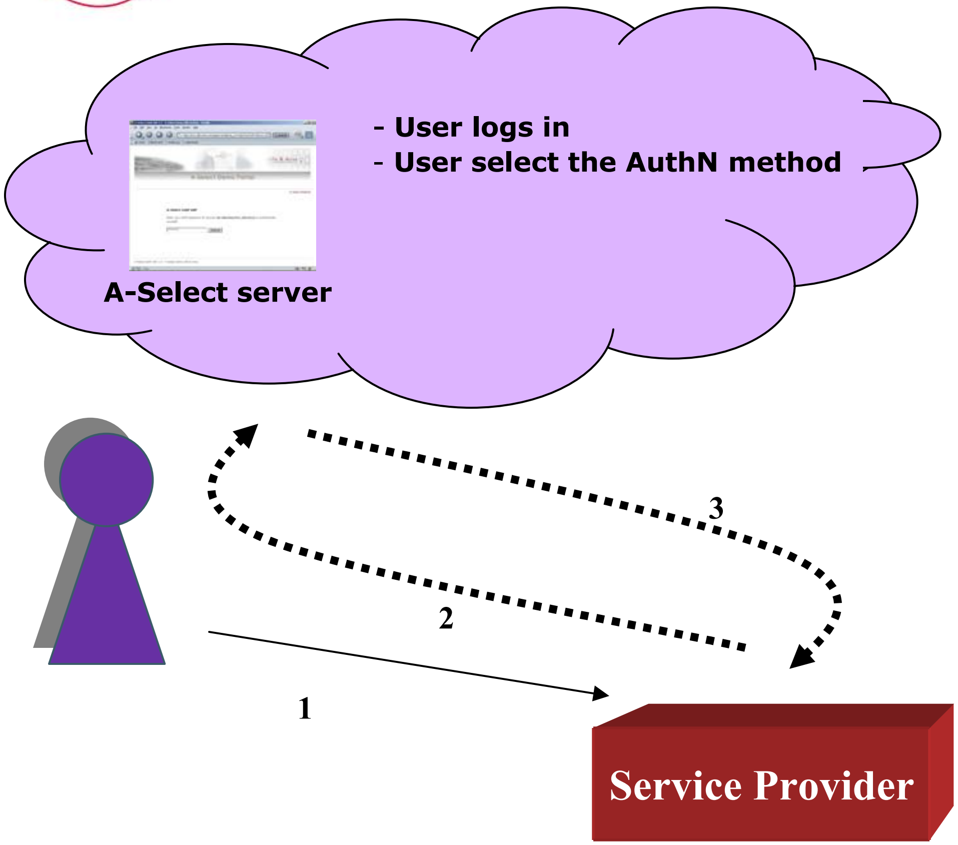
- Based on implementing the Shibboleth protocol
- Compatibility scenarios
- Inside a PAPI-based federation
    - Incorporate an IdP
    - Incorporate a SP
    - Inside a Shibboleth-based federation
    - Incorporate a PoA
    - Incorporate an AuthServer
- Validated against test facilities
    - http://www.testshib.org

Courtesy of Diego Lopez (RedIRIS)

SSO Systems: A-Select

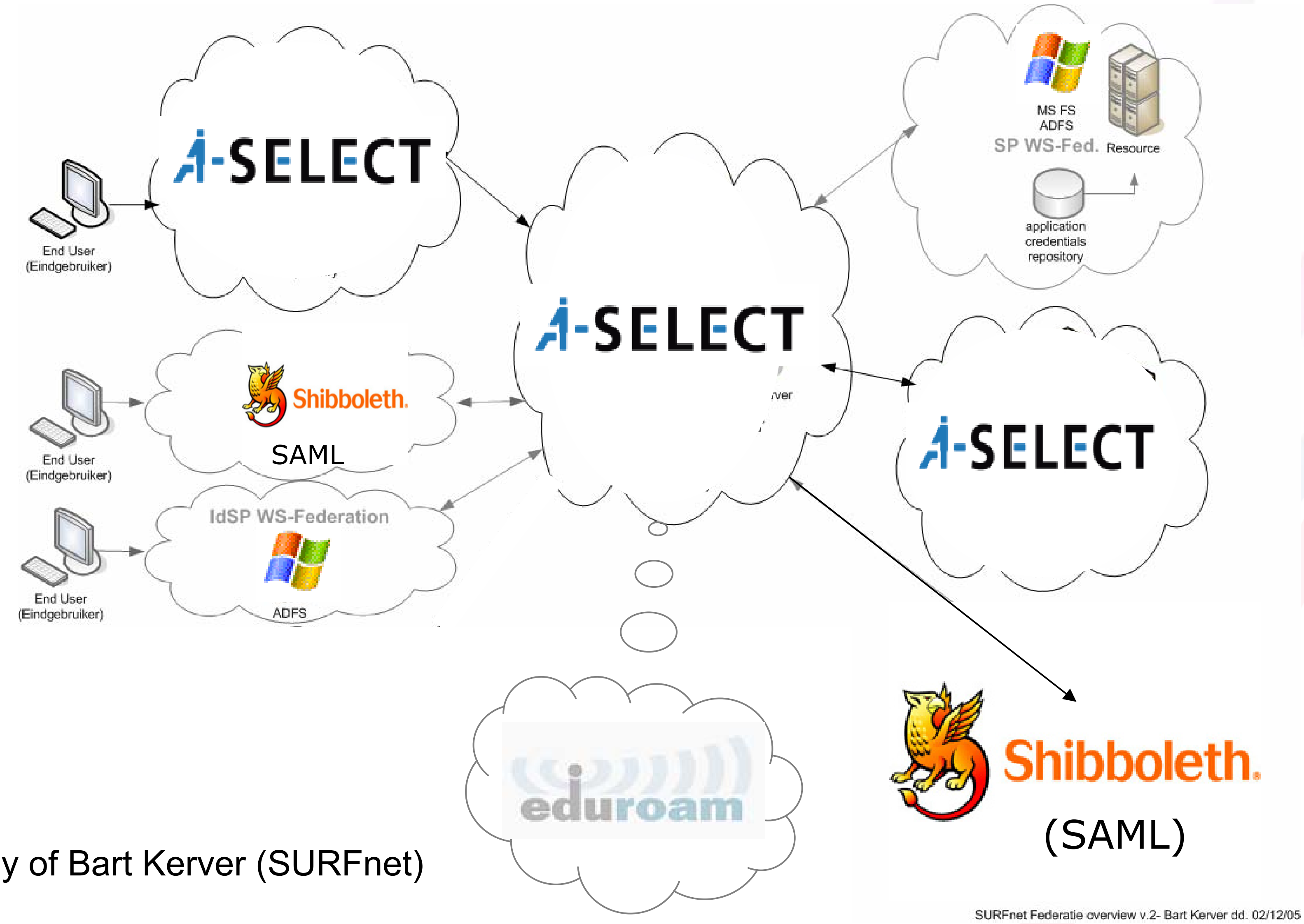
- A-Select allows for authentications and authorization of users in a (federated) Web environment
  - Access to a resources is granted upon users' authentication at their home institutions: "authenticate locally, act globally";
- Users identify with the A-Select server
  - Several authentication methods are possible ("authN strength");
  - The user authN method is added to the user's assertion;
  - Applications decide which method of authentication is needed.
- A-Select is compatible with SAML1.1 (fe. Shibboleth) and Microsoft WS-Federation/ADFS; A-Select acts as a broker/translator between federation protocol assertions;

A-Select scenario



- User wants to access a A-select (or Shibboleth or WS-Federation) protected resource;
- The resource redirects the user to his/her A-Select Service;
- User's A-Select Server redirects the user to the right A-Select Authentication Service Provider (AuthSP);
- Upon authentication, A-Select Server issues a ticket for the user and asserts credentials (attribute release);
  - User is redirect to the resource

SURFfederation on A-Select



SURFnet Federatie overview v.2- Bart Kerver dd. 02/12/05

courtesy of Bart Kerver (SURFnet)

users identities central federation components resources

A quick look at the future

- Different solutions:
  - Same ultimate goal
- *Lingua franca*
  - Syntax: SAML profiles
    - Converging to 2.0
  - Semantics: eduPerson, SCHAC
- Trust fabric
  - Public key technologies (if not infrastructures)
  - Component identifiers and registries
  - Metadata repositories

- Federating federations: confederations

The First European Confederation: eduroam

- eduroam
  - Federation of national eduroam federations
  - To provide network access between the institutions connected to eduroam
- eduroam technology
  - 802.1X + RADIUS
- eduroam policy
  - Defined by GÉANT2/JRA5/TF-Mobility

- Inter-operability between eduroam and SAML-based federations being worked on via DAMe project
  - DAME = **D**eploying **A**uthentication **M**echanisms for federated service in **e**duroam architecture

GÉANT2 work: eduGAIN

- An eduGAIN confederation is a loosely-coupled set of cooperating identity federations
  - That handle identity management, authentication and authorization using their own policies
- Trust between any two participants in different federations is dynamically established
  - Members of a participant federation do not know in advance about members in the other federations
- Syntax and semantics are adapted to a common language
  - Through an abstract service definition

TERENA Role

- TERENA not involved in deploying federation
  - TERENA will join SURFnet federation

- TERENA provide support and coordination for the international activities
- Via Task Forces
  - TF-EMC2
  - Next TF-EMC2 meeting in Florence (28-29 March)
  - TF-Mobility
- And related sub-groups
  - REFEDS
  - ECAM (European Committee for Academic Middleware)
- Workshops
  - EuroCAMP
  - Next EuroCAMP April 17-18 Helsinki

REFEDS

- REFEDS: Research and Education Federations
- Aim of the group: discuss technical specifications as well as policies to define procedures and guidelines to allow for interoperability of federations.

- REFEDS Wiki:
  - Survey of current federations
  - http://www.rediris.es/wiki/tf- emc2/index.php/Federations

Conclusions

- There will not be one unique multipurpose federation
  - Different federations to fit different communities

- What technology to use for your federations?
  - It really depends on your needs

- What are your requirements?
  - What kind of services do you want to offer?
  - Do you plan to provide Web Single Sign On only?
  - Do you need a strong user support?
  - Do you need strong authentication?

- Ultimately it does not really matter what you choose as long as you go for standard-based (SAML) solution

Links

- TF-EMC2
  - http://www.terena.org/activities/tf-emc2/
- REFEDS
  - http://www.terena.org/activities/refeds/
- eduroam
  - http://www.eduroam.org/
- GÉANT2/JRA5
  - http://www.geant2.net/server/show/nav.758
- DAME project
  - http://dame.inf.um.es/htmldocs/dame_sso.html
- PAPI
  - http://papi.rediris.es/
- A-Select
  - http://a-select.surfnet.nl/